White Paper

Lightweight M2M 1.1:

Managing Non-IP Devices in Cellular IoT Networks

Sergey Slovetskiy, T-Mobile
Poornima Magadevan, T-Mobile
Yun Zhang, Ericsson
Sandeep Akhouri, Ericsson

October 2018

Executive Summary

OMA Lightweight M2M 1.1 (LwM2M 1.1) standard provides device management and service enablement capabilities for managing IoT devices in Cellular Internet of Things (Cellular IoT) networks. Based on 3GPP standardization, Low Power Wide Area (LPWA) functionality can be provided on Narrow-Band IoT (NB-IoT), Cat-M1 and Extended Coverage GSM IoT (EC-GSM-IoT) bringing major enhancements to low-cost and simplified devices with extended coverage and long battery life. In Cellular IoT networks, Service Capability Exposure Function (SCEF) can securely expose the services and capabilities of 3GPP network interfaces via standardized API for managing devices. This includes supports for Non-IP Data Delivery (NIDD), Communication Patterns (CP), Monitoring Event (MONTE), Triggering, and other enhanced features introduced by 3GPP to facilitate Machine Type Communications (MTC, Ref [10]).

This whitepaper discusses the capabilities introduced in LwM2M 1.1 for managing non-IP devices in Cellular IoT networks, more specifically, supporting NIDD over NB-IoT. LwM2M 1.0 supported UDP and SMS transport bindings. LwM2M 1.1 adds support for the "non-IP" transport. LwM2M 1.1 also introduces more efficient data formats, optimized message exchanges, and support for application layer security based on Object Security for Constrained RESTful Environments (OSCORE), (Ref. [8]). These LwM2M 1.1 features can significantly improve the performance and security for non-IP devices in lossy and low bandwidth networks such as NB-IoT. Standardized LwM2M objects and resources defined for NB-IoT networks also provide inter-operability for standard information reporting and device management capabilities across device Original Equipment Manufacturers (OEMs).

1. Introduction

This document begins with outlining Operator motivation and IoT development challenges faced by partners & application developers when deploying IoT devices in cellular networks. It further elaborates on the E2E device ecosystem, vendor interoperability, and security considerations.

Section 3 provides an overview of the new features in LwM2M 1.1 that support non-IP devices in Cellular IoT networks, and discuss the significant features, performance, and security enhancements.

Section 4 discusses Non-IP Data Delivery (NIDD) over Service Capability Exposure Function (SCEF). It briefly covers the evolution from SCEF to NEF (Network Exposure Function) in 5G.

Section 5 summarizes the advantages of using LwM2M 1.1 in Data & Device Management for IoT devices in NB-IoT networks. It provides guidance on managing non-IP devices, switching between multiple transports, and performing secure firmware updates, and discuss standard LwM2M objects and resources relevant in NB-IoT.

2. Operator Motivation and IoT Development Challenges

2.1. Narrowband IoT (NB-IoT)

NB-IoT is the mobile radio access technology targeted at low-cost support for massive deployment of lightweight and constrained IoT devices. As such, it has the characteristics of the constrained network. It can operate in a system bandwidth as narrow as 180 kHz and supports deployment both in spectrum originally intended for GSM or LTE (Ref. [11]). NB-IoT devices can support multiple Power Saving Modes, including PSM, extended I-DRX, and C-DRX. In addition to data transmission, the overlaying protocols must also efficiently address the low-level fragmentation for large data transmissions.

NB-IoT can be used in both IP and non-IP modes. Application Developers need to account for the data transmission efficiency and minimize the overhead of the data transmitted over the Cellular IoT network.

2.2. NB-IoT Hourglass

NB-IoT brings new challenges of fitting the IoT data communication from constrained devices into a constrained communication channel:

- Narrow band
- Low frequency of communications
- Small payload
- High latency
- Devices typically sleeping most of the time

The main challenge becomes - how to eliminate the overhead of IP and TCP/TLS.

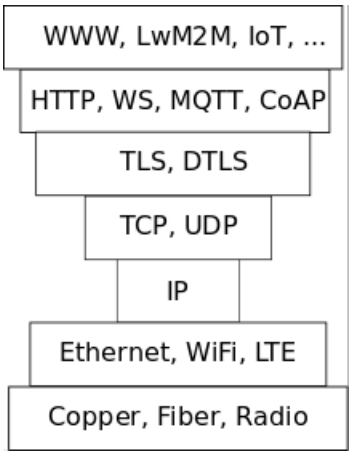
The device classes targeted by the Cellular IoT and, by NB-IoT technologies transmit single byte to 10s of bytes in one payload. The devices are supposed to be in sleep mode most of the time, and there are strong limitations imposed by the network on this highly streamlined data transmission channel. Typically, the bandwidth will be around 10s of kbps. The payload must fit in the radio frame. Devices are supposed to be transmitting with very low frequency - at most several times per hour, and the transmission latency may be very high (Ref [11][12]).

These limitations are challenging for the industry used to the relative freedom of modern high-end communications channels, which even on Cellular Radio (LTE) delivery with 10s of Mbps bandwidth, latency from 10s to 100s of milliseconds, and reliable long-lived TCP connections that are always available. With the effective payload to the magnitude of bytes or at most 10s of bytes, the overhead introduced by the TCP/IP stack becomes significant.

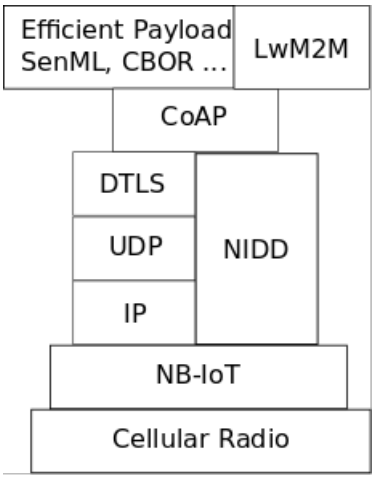
NB-IoT allows constrained devices to overcome this limitation by introducing the “Non-IP” Transport, and therefore eliminating the TCP/IP stack completely. However, this poses the new challenge for Application Developers on how to address the need to manage payload fragmentation, in-order delivery, and flow control.

Combination of NB-IoT with the technologies constituting the LwM2M 1.1 stack effectively address those challenges and allows smooth transition to the Constrained IoT Stack, which can also be called the "NB-IoT" stack. The data can be delivered efficiently, and also the devices themselves can be efficiently managed by the LwM2M Device Management functionality, allowing for remote, low maintenance, long battery life device deployments and other solutions.

Web Model: **1000s of bytes**



Constrained IoT Model: **1s to 100s of bytes**



In this model, CoAP (Constrained Application Protocol) based protocols such as LwM2M become new spanning technology. With built-in congestion control, block-wise transfer fragmentation handling mechanism, efficient coding of headers and payload, and being effectively transport agnostic, CoAP-based LwM2M stack can be reused for both IP- and Non-IP- based NB-IoT deployments.

2.3. Device Ecosystem

An increasing number of connected devices is expected to be introduced in coming years. As a result, to automate and monitor a medium sized factory, the initial device deployment would require a significant investment. To keep the costs low and increase the adoption of these connected devices, low power consuming and constrained devices are increasingly being enabled in the market. These devices are designed to address a specific purpose, for example, a small sensing device just to collect and transmit raw data, rather than a highly capable device with full in-built computing to perform data analysis in place. These devices are expected to be in operation for years with zero to very low maintenance to keep the operation cost as low as possible. Such device deployment practice requires longer battery life, minimal remote device updates, and capabilities to perform remote device monitoring and maintenance. In order to conserve devices and network resources, these devices are expected to be in sleep mode for majority of their lifetime.

These devices are expected to be programmed once with basic set of functionalities (for example, sensor readings), and then they can run for many years in sending minimal amount of data (for example, a few bytes at a time) to backend systems. OEMs are diligently working towards optimization of the frequency of transmissions and data models of these devices.

For some of these devices, an IP header itself is redundant for a packet compared to the actual payload. Non- IP communication provides a happy medium here and is a well-suited transport for such devices. With the increase of market fragmentation, solution providers, and conflictive requirements, OEMs need a “standard” based implementation for providing necessary security and need the reuse of a common device framework to efficiently enable various use cases. LwM2M standard together with the new transport bindings introduced in LwM2M 1.1 provides an excellent option for the OEMs to leverage a consistent efficient standard architecture for data transmission.

2.4. Vendor Inter-operability

Market adoption for end-to-end IoT solutions is increasing, which leads solution providers to mix and match different technologies according to their use cases to reach the final product offering. The combination of constrained devices and high-end implementations is seen repeatedly in market deployments. To keep solutions robust, secure, and low costed, solution providers are continuously optimizing devices and their communication patterns, as well as introducing intelligence at the edge.

With varied use case opportunities from smart cities to home automation, reusable becomes a key requirement from a solution provider’s point of view. Configurable software model reduces software development timelines and repurposes device hardware with minimal changes across different use case implementations. It quickly becomes an essential requirement to be able to scale solutions across wide-spread market demands. Solution providers are looking for opportunities and standardization in terms of resource reuse, configurable parameters, and so on.

The wide mix of solutions and implementations across the industry poses a challenge in enabling a set of use cases that span across multiple devices/servers. This limits the scalability and expansion of different portfolio of use cases. The typical implementation of industrial automation would warrant multiple devices to work together. The type of sensors and edge computing is determined by the factors, such as physical location of the industry, its environmental setting, and weekly/daily output scale, to enable the solution. An industrial automation solution of this scale would require the capability of continuous observations of any value changes that are followed by updates reliably communicated to central application. LwM2M provides a standard structure with well-defined objects to enable this mix of use cases, devices, and so on, which makes the application implementation consistent with a standard operating model.

2.5. Security

Security of data communication, especially device provisioning and management operations, is critical for IoT solutions. LwM2M already supports various modes of DTLS-based Transport Layer Security. However, the usual TLS handshake exchange and crypto operations add overhead to both traffic over the air and resource utilization of constrained devices.

The considerations, such as each byte, compute cycle and transmission over the air count, are critical for the NB-IoT networks.

NB-IoT network itself provides the air link encryption, which is coupled with the managed data path via an operator with controlled SCEF and NEF and ensures the protection of the data transmitted via the 3GPP Cellular IoT architecture in the operator domain.

More security-demanding IoT applications can be benefit from the Payload/object-level security based on IETF COSE (Ref [7]), as introduced in LwM2M 1.1. Using lightweight credentials management mechanisms already provided by LwM2M 1.0 and extended in LwM2M 1.1, only the payload objects can be encrypted eliminating significant overhead of DTLS handshakes and the necessity to encrypt all traffic.

3. OMA Lightweight M2M 1.1

LwM2M 1.0 supported UDP and SMS transport bindings. LwM2M 1.1 introduces support for Non-IP transport bindings to enable management of devices operating in Cellular IoT Networks, including NB-IoT and LTE-M. It provides the following new features to improve maintainability, security, and performance:

- Support of LwM2M over Low Power WANs, including 3GPP CIoT and LoRaWAN
- Performance improvement for retrieving and updating Resources of multiple objects
- Support for JSON using SenML with CBOR (Concise Binary Object Representation) serialization
- Support of LwM2M over TCP/TLS to support firewall and NAT traversal
- Support for application layer security for LwM2M based on OSCORE
- Enhanced registration sequence mechanisms by the LwM2M Client
- Enhancement of the bootstrapping capabilities allowing for incremental upgrades
- Extended LwM2M commands to enable Resource Instance level access
- Improved support for Public Key Infrastructure (PKI) deployment
- Addition of new Data Types

In this section, we discuss LwM2M 1.1 features relevant to NB-IoT in more details.

3.1. Non-IP Transport Binding

LwM2M 1.0 provided support for UDP and SMS. LwM2M 1.1 protocol stack illustrated in Figure 1 provides support for TCP, CIoT, and LoRaWAN. UDP, SMS, and CIoT transports can be used with or without DTLS. TCP can be used in conjunction with TLS.

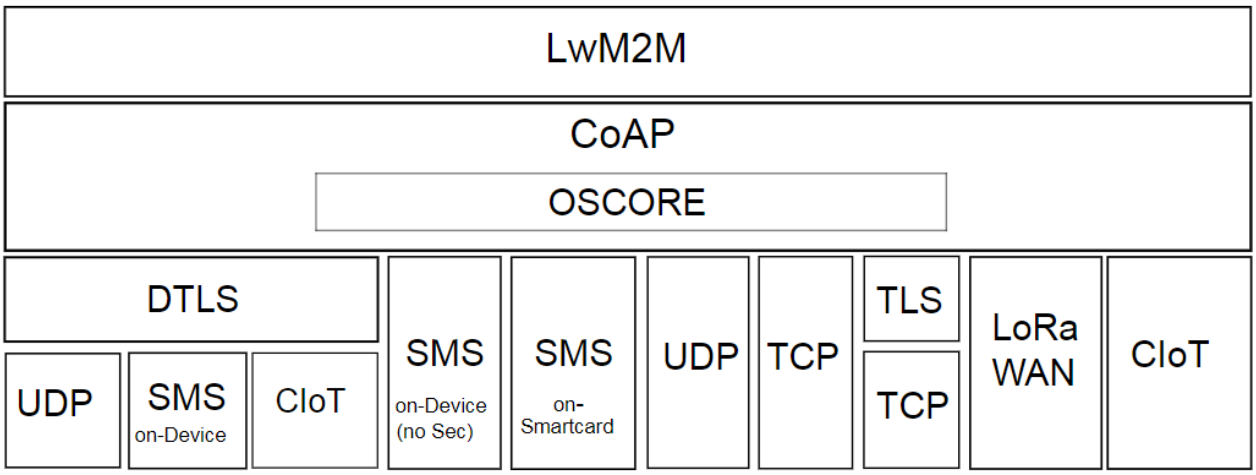


Figure 1: LwM2M 1.1 Protocol Stack

LwM2M 1.1 also supports OSCORE, an application layer security protocol that enables support for proxy operations and end-to-end security independent of underlying transport layer protocols. OSCORE can be used with any of the transport bindings, including UDP, SMS, and TCP, with or without DTLS or TLS.

LwM2M 1.1 defines additional transport bindings viz. T (TCP) and N (Non-IP). Non-IP is defined in accordance with 3GPP TS 23.401 and is applicable to both NB-IoT and LTE M networks. Non-IP can also refer to alternate transports such as LoRAWAN.

3.2. Queue Mode and Device Triggers

LwM2M 1.0 defines Queue Mode and SMS triggers as part of the Current Transport Binding resource. For example, the 'UQS' transport binding, which indicates support for the UDP-based transport with both Queue Mode and SMS based device triggers.

LwM2M 1.1 decouples Queue Mode and Trigger from the Current Transport Binding. The Queue Mode can be enabled independently of the underlying transport. During the registration process, the device indicates its supports for queue mode by including "Q" in the registration parameters upon initial registration.

The support for SMS based triggers, can be indicated by the 'Trigger' resource that has been included as an optional resource on the LwM2M Server Object. An LwM2M Client that can be reached over an SMS binding or supports SMS Registration Update Trigger, should indicate the MSISDN or external identifier for the 'SMS Number' parameter as part of its registration parameters during initial registration. In case of SMS based triggers, and unlike the SMS bindings that require a response over SMS, no response is expected from the device.

As mentioned earlier, NB-IoT devices can support multiple Power Saving Modes, including PSM, extended I-DRX, and C-DRX. To support the sleep mode behavior, Queue Mode and SMS-based device triggers help conserve valuable network and device resources. 3GPP SCEF architecture (Figure 5) includes the support for Device Triggering over T4 interface. In addition, SCEF can also provide buffering capability to queue requests for NB-IoT devices.

Since the network can effectively override the PSM values for a device, IoT devices need to effectively communicate their sleep duration to the LwM2M Servers to prevent de-registration. The LwM2M Client must send a registration update to extend the lifetime of the registration based on the configured PSM values.

3.3. Server Initiated Bootstrap & Bootstrap Read

In LwM2M 1.1, Server Initiated Bootstrap Mode has been modified to simply allow the Bootstrap Server to trigger the device to invoke Client Initiated Bootstrap Mode. Server Initiated Bootstrap thereby provides a simple and reliable way for the LwM2M Server to initiate a Bootstrap Sequence, while reusing the proven Client Initiated Bootstrap mechanism.

Server Initiated Bootstrap Mode uses a *Bootstrap-Request Trigger* resource (/{Object ID}/{Object Instance ID}/{Resource ID}/1/1/9), an optional resource defined on the LwM2M Server Object, to initiate a request to the LwM2M Bootstrap-Server account that is pre-configured on the device.

A Bootstrap Read operation is introduced to allow for the Bootstrap Server to query the existing Server Accounts and add/remove new Server Account(s) without breaking the Access Rights that are already in place for the targeted LwM2M Client. The only acceptable targets for the Bootstrap Read is the LwM2M Server Object (Object ID: 1) and the Access Control Object (Object ID: 2).

Server Initiated Bootstrap can be a valuable feature as it can be integrated with Automatic Device Detection component in Operator networks to onboard devices. It can be used to reset credentials for devices. Bootstrap Read operation allows Operators to closely manage and monitor devices while providing flexibility to support the LwM2M objects that are managed by device OEMs or external application vendors.

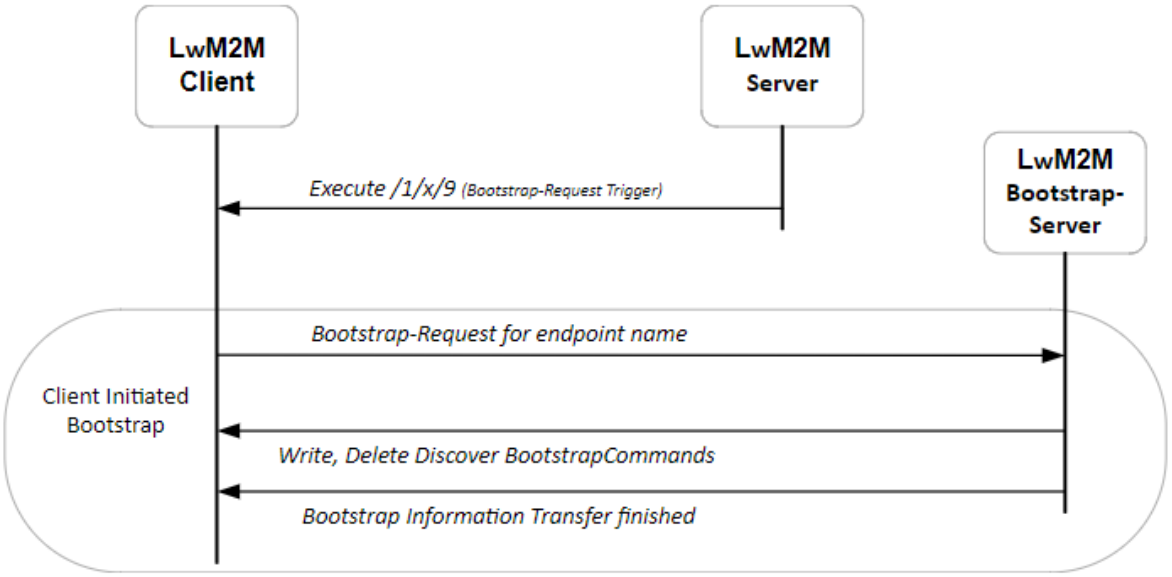


Figure 2: Server Initiated Bootstrap

3.4. Optimized Data Formats & Efficient Messaging

LwM2M 1.1 provides support for compact data format for information exchange along with support for efficient encoding and decoding. In addition to the previously supported Opaque, Plain Text, TLV, and JSON data formats, LwM2M 1.1 introduces support for JSON using SenML with CBOR serialization for compressed payload to enable highly efficient data transmission.

LwM2M 1.1 also provides performance improvement for retrieving and updating Resources of multiple objects. Several "Composite" operations are introduced for reading, writing, and observing resources and resource instances across LwM2M objects in a single request. This allows the LwM2M server to access a subset of resources in an instance or across instances of the same or different objects within a single request instead of issuing multiple requests.

The Read-Composite operation can be used by the LwM2M Server to selectively read several Resources, and/or Resource Instances of different Objects in a single request. The list of elements to be read are provided as separate parameters to the operation in JSON/CBOR format. The format is similar to JSON/CBOR reply format, but there is no values for the resources.

The Write-Composite operation can be used by the LwM2M Server to update values for several different Resources across different Instances of one or more Objects. This Write-Composite operation is in contrast to the standard Write operation, the scope of which is limited to a Resource(s) of a single Instance of a single Object. Similar to Read-Composite, the Write-Composite operation provides a list of all resources to be updated, and their new values, using the JSON/CBOR format.

The Observe-Composite operation can be used by the LwM2M Server to initiate observations for a group of resources and/or resource instances across multiple object instances within the client. As with the Read-Composite operation, the list of elements to be observed is provided as separate parameters to the operation in JSON/CBOR format.

In LwM2M 1.0, multi-Instances Resources could only be addressed as a whole. In LwM2M 1.1, individual Read and Write accesses on a certain Instance of an LwM2M Multi-Instances Resource are also supported through Device Management and Service Enablement Interface.

3.5. Security Enhancements

The LwM2M protocol requires that all communications between LwM2M Clients, LwM2M Servers, and LwM2M Bootstrap-Servers to be mutually authenticated, encrypted, and integrity protected. Since LwM2M 1.1 adds support for TCP, both DTLS and TLS can now be used in secure communication.

LwM2M 1.1 provides alignment with current security practices and better performance with new TLS/DTLS extensions. Additionally, it provides recommendations for certificate revocations, integration with already deployed CA infrastructure, and so on,

LwM2M Server Object also provides capabilities via optional resources to improve the error handling behaviour during bootstrapping and registration.

3.5.1 Object Security for Constrained RESTful Environments (OSCORE)

LwM2M 1.1 specification supports application layer security protocol, such as OSCORE. OSCORE protects CoAP message exchanges and is applicable to protocol messages which can be mapped to CoAP or a subset of CoAP, including HTTP and LwM2M. OSCORE enables support for proxy operations and provides end-to-end security independence for underlying transport layer protocols. OSCORE can be used in any transport bindings, including UDP, SMS and TCP, with or

without DTLS/TLS. It can be used between LwM2M endpoint and non-LwM2M endpoint, for example, between an Application Server and an LwM2M Client. In this case, an LwM2M server thereby provides E2E security for communications over intermediate nodes.

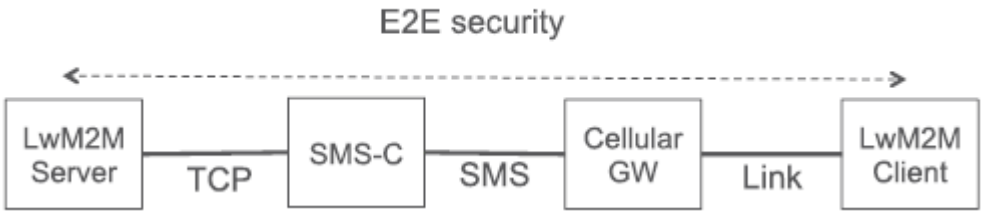


Figure 3: Example of E2E Security over varying Transport

LwM2M 1.1 adds a core LwM2M OSCORE (ID:21) object. The LwM2M Security Object, OSCORE security mode is an optional resource that links to the LwM2M OSCORE object instance. Similar to the LwM2M Security Object, the LwM2M OSCORE Object must only be accessible and updatable by one LwM2M Bootstrap-Server.

The OSCORE LwM2M Object provides the key material and related information of an LwM2M Client to access the specified LwM2M Server. The OSCORE LwM2M object includes resources to identify Master Secret, Sender ID, Recipient ID, AEAD Algorithm, HMAC Algorithm, and Master Salt.

4. 3GPP Cellular IoT

3GPP has embraced several LPWA (Low Power Wide Access) technologies, such as NB-IoT, CAT-M1, and so on, to address the requirements of low power and long battery life. The power-hungry protocol for establishing IP data bearers has been replaced by extending the NAS protocol to allow small amounts of data to be transferred over the control plane. The IP stack is not necessary, hence, this type of data transfer is referred to as NIDD (Non-IP Data Delivery). Figure 4 displays the path for NIDD between UE and AS traversing the MME and SCEF.

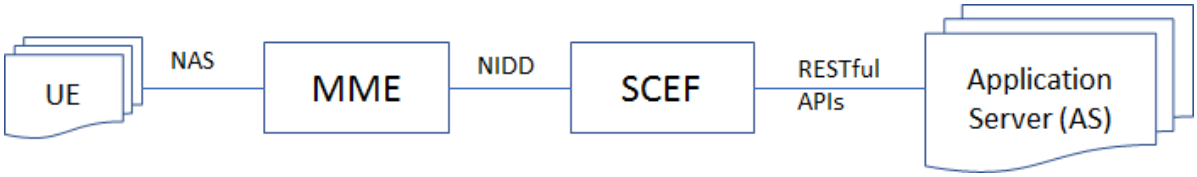


Figure 4: Non-IP Data Delivery

4.1. Service Capability Exposure Function (SCEF)

SCEF introduced in 3GPP R13 TS 23.682, provides a way to securely expose the services and capabilities of 3GPP network interfaces. SCEF facilitates the operators to exposes the capabilities of networks, such as Charging.

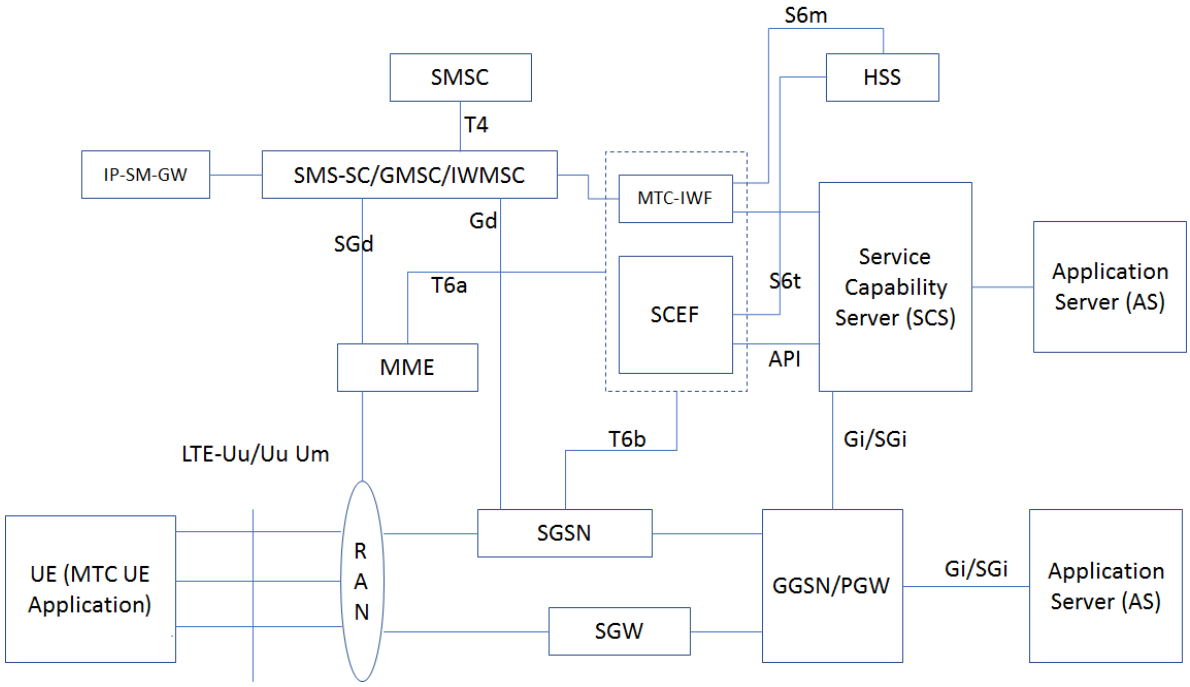


Figure 5: Service Capability Exposure Function

SCS is the entity which connects MTC application servers to the 3GPP network to enable the application servers to communicate through specific 3GPP-defined services with UEs that are used for MTC. SCS communicates with SCEF using standardized APIs.

4.2. Network Exposure Function (NEF)

The following architecture assumptions and principles are applicable for Cellular IoT support and evolution in the 5G System:

- NB-IoT or CAT-M1 is connected to 5G Core (5GC)
- No architectural enhancements made to Evolved Packet Core (EPC)
- APIs for Cellular IoT related services provided to SCS/AS shall be common for UEs connected to Evolved Packet System (EPS) and 5GS
- Support for small data delivery using IP data and Unstructured (Non-IP)
- At least equivalent level of security for UEs used for Cellular IoT in 5GS system as in EPS

Network Exposure Function (NEF) inherits functions from SCEF. NEF introduced in TS 23.501 is the key entity within the 3GPP architecture to securely expose the services and capabilities to

Application Servers, which are provided by 3GPP network interfaces through Application Programming Interfaces (APIs).

4.2.1 Small Data Delivery

The 5G System is assumed to support functions for small data communication corresponding to 4G EPS. Small data communication includes infrequent and frequent small data transmissions aiming to support efficient small data transmissions for Cellular IoT, for example, tracking devices for both Mobile Originated (MO) and Mobile Terminated (MT) use cases. It is expected that the number of such devices can increase exponentially, but the data size per device will remain small.

These EPS functions are also known as Non-IP Data Delivery (NIDD) procedures and involve transmission either using the T8 API or directly over the SGi.

4.2.2 Common North-bound APIs for EPC-5GC Interworking

When a UE is capable of switching between EPC and 5GC, it shall only be associated with combined SCEF+NEF node(s) for Service Capability Exposure. The SCEF+NEF hides the underlying network topology from the AF (such as SCS/AS) and hides whether the UE is served by 5GC or EPC. The following figure shows the SCEF+NEF architecture.

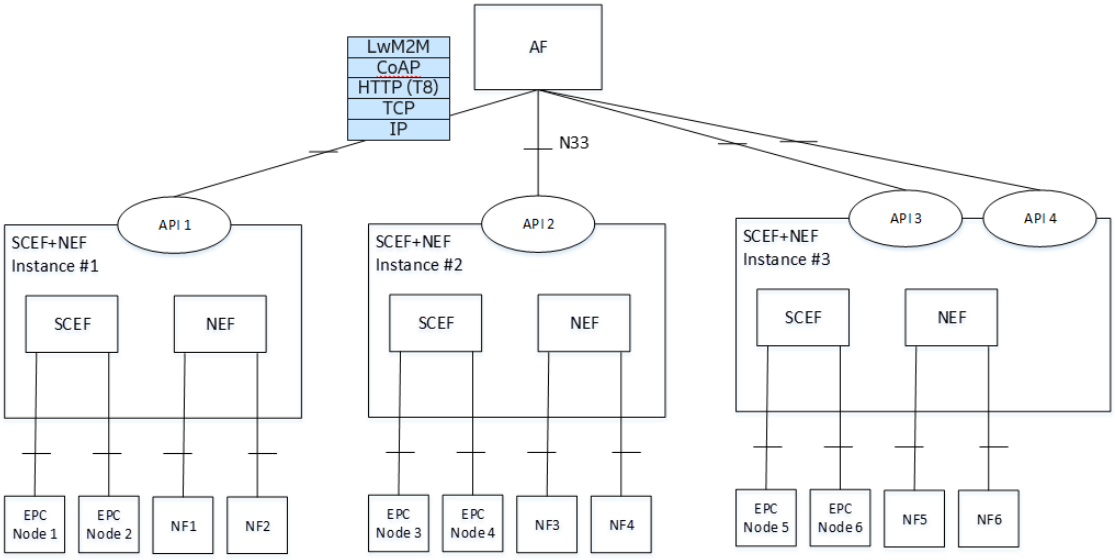


Figure 6: SCEF + NEF Architecture

The API interface that is exposed by the SCEF+NEF interface is a N33/Nnef interface that supports the 3GPP T8 APIs (refer to TS 29.122). LwM2M over CoAP may be embedded in T8 APIs as the delivered data payload.

5. Managing Non-IP Devices in Cellular IoT Networks

Non-IP Transport Binding is applicable to both NB-IoT and LTE-M networks. Non-IP can also refer to alternate transports such as LoRaWAN. Non-IP data transfer over UP utilizing the IP Tunnel is transparent to the AS since the non-IP device has an "IP" assigned by C-SGN. Non-IP data delivery (NIDD) over SCEF can include LwM2M/CoAP payload.

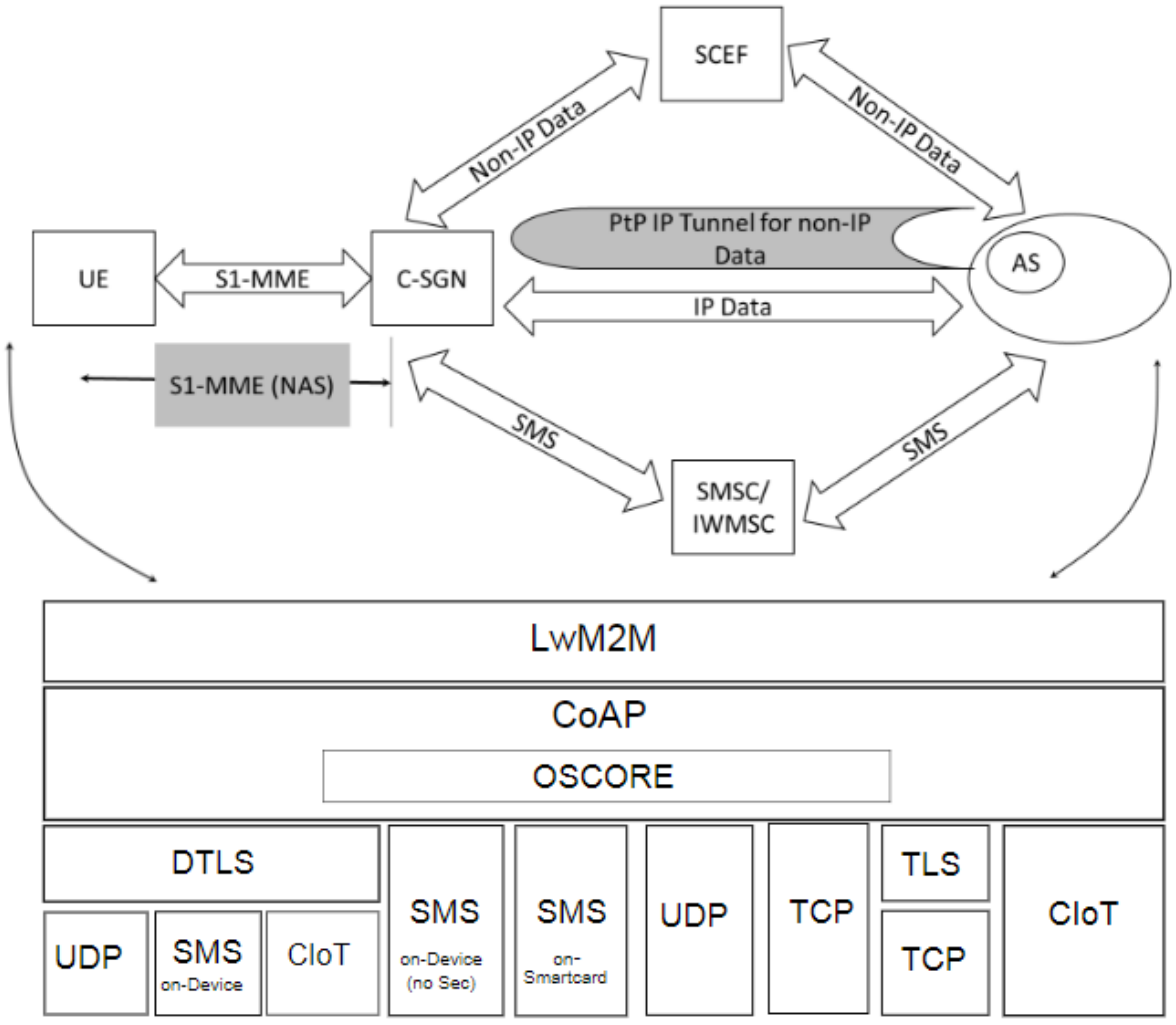


Figure 7: LwM2M over Cellular IoT

5.1. External Identifier

According to 3GPP TS 23.628, "*the User Identity (IMSI) shall not be used on the interface between SCEF and SCS/AS"*, the SCS/AS shall use MSISDN or External Identifier to identify a user in order to perform NIDD configuration or to send/receive NIDD data. In order to facilitate correlation of SCS/AS requests to T6a/T6b connection for a given UE, the HSS provides the user's IMSI to SCEF. The MSISDN (when NIDD Configuration Request contains an External Identifier) and External Identifier (when NIDD Configuration Request contains an MSISDN) are also provided if available.

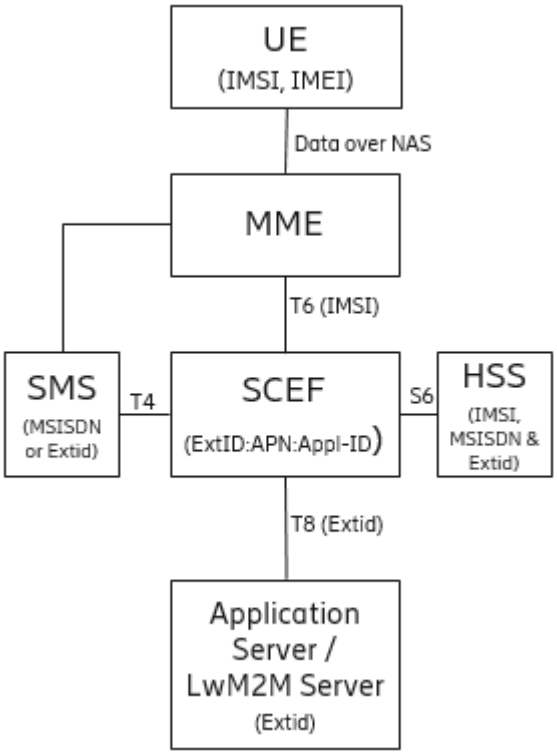


Figure 8: External ID in SCEF

LwM2M 1.1 supports Network Access Indicator (NAI) URN to identify devices using a combination of "Local Identifier@Domain Identifier" as defined in 3GPP TS 23.003.

Examples:

- The NAI 123456789@domain.com is represented as urn:nai:123456789@domain.com.
- The NAI user@homerealm.example.net is represented as urn:nai:user@homerealm.example.net.

SMS also supports external identifiers besides MSISDN.

Based on User Identity confidentiality security mechanism described in '*Security architecture and procedures for 5G system*', Subscription Permanent Identifier (SUPI) shall not be sent outside the 3GPP operator domain that is secured by 5GC Network Exposure Function and should map to External Identifier.

5.2. Registration Update Trigger

When the LwM2M Client has registered to an LwM2M Server, the LwM2M Server can make the LwM2M Client update its registration by executing the Registration Update Trigger Resource in the matching Server Object Instance. The following is an example flow of triggering the LwM2M Client in Queue Mode to send the updated message to the LwM2M Server regardless of offline status. POST /1/x/8 brings the LwM2M Client online to connect to the LwM2M server. The variable x indicates the right instance pointing to the server.

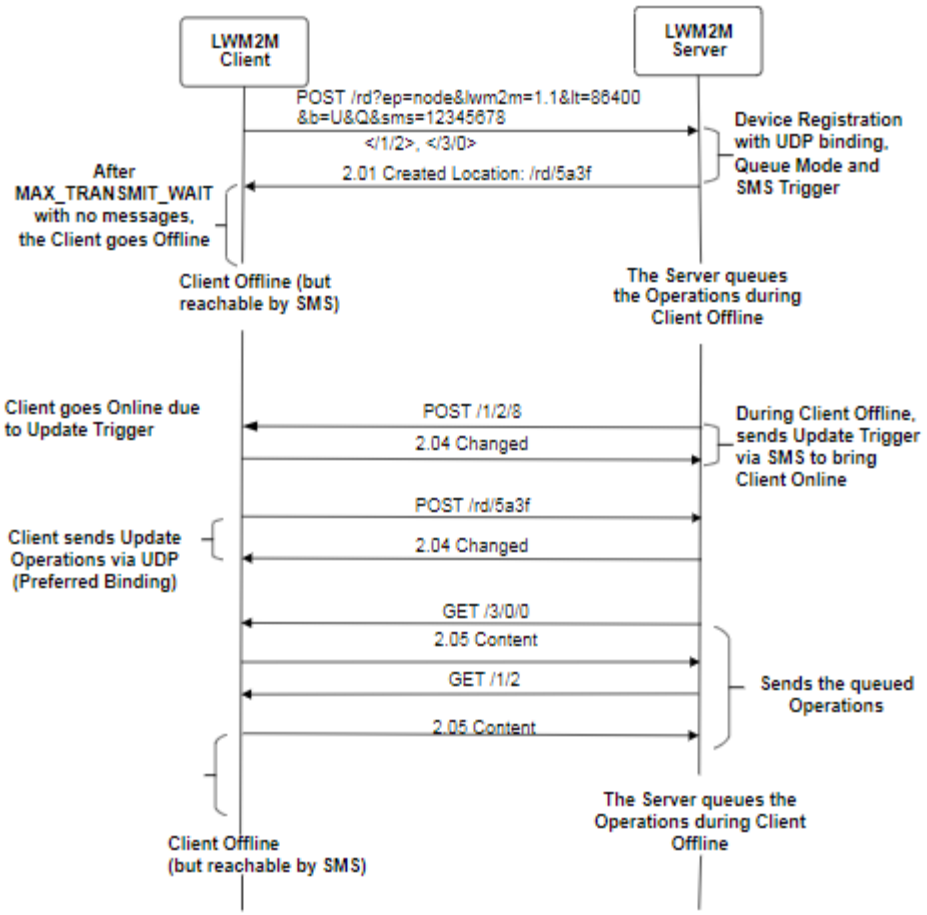


Figure 9: Example of Registration Update Trigger

In LwM2M 1.1, a transport parameter can optionally be included in the Registration Update Trigger, for example, *POST /1/x/8?0=U*. Upon the received trigger, the LwM2M Client may use the UDP transport binding to reconnect to the LwM2M Server.

5.3. Preferred Transport

Preferred Transport is an optional resource in the LwM2M Server Object. If this resource is defined, the device may use this to initiate a connection over the specified transport. This resource can be used to switch between multiple transports, for example, a non-IP device can switch to UDP transport to perform firmware updates. If this resource is undefined, the default mode is implemented.

While multiple transports are supported, only one transport binding can be used during the entire session. For example, when both UDP and SMS are supported, the LwM2M Client and Server can choose to communicate over either UDP or SMS during the entire session.

5.4. Firmware Updates

The LwM2M Client and Server support block-wise transfer if they implement the Firmware Update object. For constrained devices, it is recommended to use CoAP for firmware downloads. However, protocols such as HTTP/HTTPS, can also be used for downloading firmware updates (via the Package URI resource). LwM2M 1.1 also includes support for CoAP over TCP and TLS (RFC 8323).

In order to support secure fragmentation of the messages between LwM2M Server and LwM2M Client, the fragments must be verifiable separately, especially in the case of firmware updates. The specification of Blockwise Transfer is vulnerable to interchange of blocks between different requests to the same resource. An attack may occur when the replay window size of the security protocol is greater than 1, even if the requests are not interleaved. Attacks may happen to both DTLS and OSCORE. The attack does not occur when a connection-oriented transport, such as CoAP over TCP, is used, or when a replay window size of 1 is selected with DTLS.

A solution is using the CoAP Request-Tag Option for unique tagging of requests in a certain scope. The Request-Tag is analogous to the CoAP E-Tag Option. But tags only request and do not response. The LwM2M Client and LwM2M Server that support Blockwise SHOULD implement the CoAP Request-Tag Option.

5.5. LwM2M Objects & Resources

LwM2M objects have been enhanced to accommodate devices operating in NB-IoT networks. Multiple device OEM can use LwM2M resources defined as part of standard LwM2M objects to capture the NB-IoT specific resources.

More details on these LwM2M Objects and associated resources are as follows.

- Connectivity Monitoring (urn:oma:lwm2m:oma:4)

In Connectivity Monitoring Object, the Network Bearer can contain the NB-IoT (5). The Link Quality Resource can also contain the received link quality, for example, NRSRQ for NB-IoT.

  - Monitoring parameters related to network
  - Network Bearer (NB-IoT): Radio Signal Strength (NB-IoT: NRSRP), Link Quality (NB-IoT:NRSRQ), and APN

- Connectivity Statistics (urn:oma:lwm2m:oma:7)
  In Connectivity Statistics Object, the Tx Data and Rx Data resources capture the transmitted or received IP data, including non-IP data.
  - Monitoring Total Amount of IP and non-IP data exchanged during a collection period

- Cellular Connectivity (urn:oma:lwm2m:oma:10)
  This object specifies resources to enable a device to connect to a 3GPP or 3GPP2 bearer, including GPRS/EDGE, UMTS, LTE, NB-IoT, SMS PSM Timer, Active Timer, and eDRX Parameter.

  - PSM Timer (10 min-992 days) - Max interval between periodic TAU if there is no other transmission from the device. During most of this time the device is considered unreachable and it can therefore go into a deep sleep mode while keeping the PDN connection(s) active.

  - Active Timer (Range: 2 sec - 31 min) - The time that the UE has to remain reachable after transitioning to idle status in case there is pending data from the NW to send out. At the end of T3324, UE can go into a deep sleep mode while keeping the PDN connection(s) active.

  - eDRX parameters for Iu/WB-S1/NB-S1/A/Gb mode – The Extended DRX parameters (Paging Time Window and eDRX value) for Iu/WB-S1/NB-S1/A/Gb mode in which the UE can send request to the network.

- APN Connection Profile (urn:oma:lwm2m:oma:11)
  This object specifies resources to enable a device to connect to an APN. The APN is also available as an objLink in LwM2M Server Object.

  - PDN Type (IPv4, IPv6, IPv4v6, non-IP), APN Rate Control.

- Bearer Selection (urn:oma:lwm2m:oma:13)
  - Preferred Communication Bearer resource is used in network selection, and if applicable, it is also used in subsequent mobility management procedures for indicating.
  - 3GPP PS LTE with Cellular IoT EPS optimizations, User Plane preferred.
  - 3GPP PS LTE with Cellular IoT EPS optimizations, Control Plane preferred.
  - 3GPP PS NB-IoT Control Plane optimizations preferred.
  - 3GPP PS NB-IoT User Plane optimizations preferred.

5.6. Non-IP Data Delivery (NIDD) with LwM2M 1.1

OMA LwM2M 1.1 protocol provides the necessary transport binding for NB-IoT devices deployed over the Cellular IoT access network. It provides highly efficient data formats and streamlined messages for lossy networks with low bandwidth. It contains the necessary semantics to perform device management and efficient data reporting.

LwM2M 1.1 supports the use of External Identifier as a valid Client Endpoint. NIDD Mobile Terminated (MT) and Mobile Originated (MO) requests can contain LwM2M payload embedded in T8 APIs between SCS/AS to Device via SCEF and MME. Data formats such on CBOR and application security based on OSCORE provide highly efficient payloads for lossy and limited-bandwidth networks. In addition to the Queue Mode, sleepy devices can also be efficiently managed by using the SMS-based Triggers that can wake up a device and also enable device to switch between transports.

Application Data can be reported using standard Information Reporting operations. In order to further conserve resources, LwM2M 1.1 also supports devices to simply send the data without observing requests. Device Management can be performed based on secure CoAP Block Transfer and alternate mechanisms.

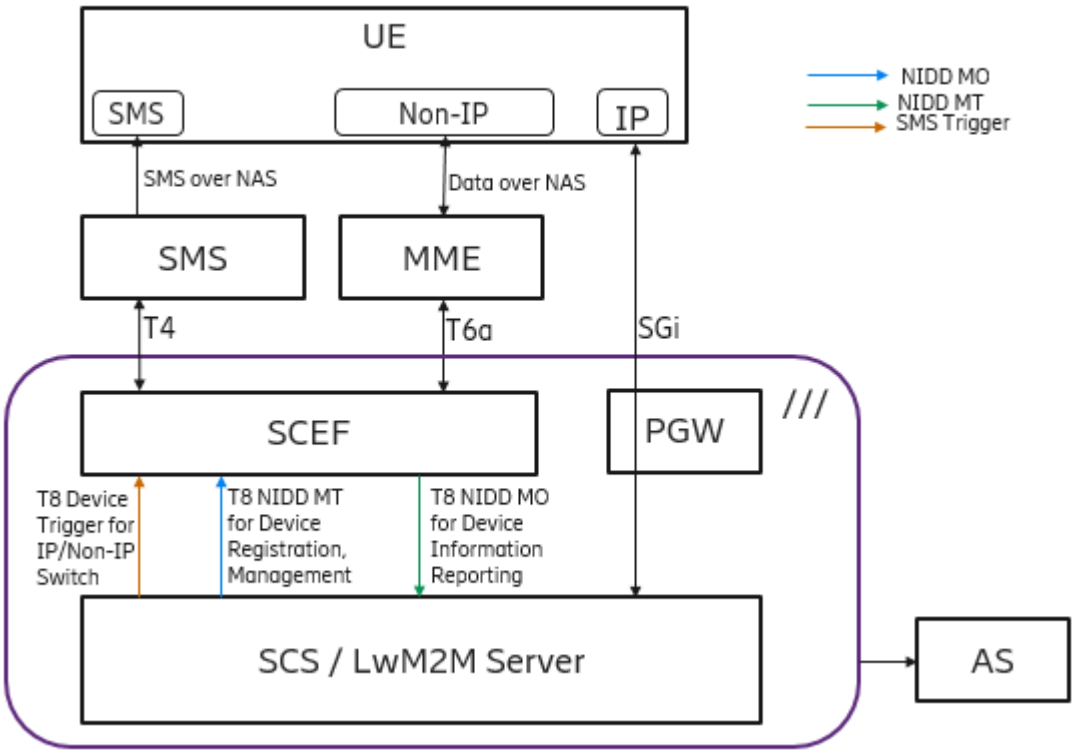


Figure 9: Support for NIDD with LwM2M

Acknowledgements

We would also like to express our gratitude to OMASpecWorks Device Management & Service Enablement Working Group chairs & member(s) for valuable feedback & comments: Padmakumar Subramani padmakumar.subramani@nokia.com, Hannes Tschofenig Hannes.Tschofenig@arm.com and Friedhelm Rodermund friedhelm.rodermund@iotecc.com

References

[1] ***[LwM2M-CORE]*** Open Mobile Alliance, "Lightweight Machine to Machine Technical Specification: Core Layer" http://openmobilealliance.org/RELEASE/LightweightM2M/V1_1-20180612-C/OMA-TS-LightweightM2M_Core-V1_1-20180612-C.pdf

[2] ***[LwM2M-TRANSPORT]*** "Open Mobile Alliance, "Lightweight Machine to Machine Technical Specification: Transport Layer"" http://openmobilealliance.org/RELEASE/LightweightM2M/V1_1-20180612-C/OMA-TS-LightweightM2M_Transport-V1_1-20180612-C.pdf

[3] ***[CoAP]*** Shelby, Z., Hartke, K., Bormann, C., and B. Frank, "The Constrained Application Protocol (CoAP)", IETF RFC 7252, June 2014

[4] ***[CoAP_Blockwise]*** C. Bormann, Z. Shelby, "Block-wise transfers in CoAP", IETF RFC 7959 - August 2016

[5] ***[CoAP_ERT]*** C. Amsuess, J. Mattsson, G. Selander, "Echo and Request-Tag", draft-ietf-core-echo-request-tag-00, Oct. 2017.

[6] ***[RFC7925]*** H. Tschofenig, T. Fossati, "Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things", RFC 7925, Jul. 2016.

[7] ***[RFC8152]*** J. Schaad, "CBOR Object Signing and Encryption (COSE)", RFC 8152, Jul. 2017.

[8] ***[OSCORE]*** G. Selander, J. Mattsson, F. Palombini, L. Seitz, "Object Security for Constrained RESTful Environments", draft-ietfcore-object-security-08, Jan. 2018.

[9] ***[3GPP TS 23.401]*** General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (EUTRAN) Access

[10] ***[3GPP TS 23.682]*** Architecture enhancements to facilitate communications with packet data networks and applications

[11] Y. P. E. Wang et al., "A Primer on 3GPP Narrowband Internet of Things," IEEE Communications Magazine, vol. 55, no. 3, pp. 117–123, Mar. 2017.

[12] ***[3GPP TS 45.820]*** Cellular system support for ultra-low complexity and low throughput Internet of Things (Cellular IoT)

About the Authors

Sergey Slovetskiy, T-Mobile US, Inc.

Sergey Slovetskiy is a Principal Engineer responsible for the Internet of Things architecture with T-Mobile US, Inc.. He worked extensively with the Open Mobile Alliance (OMA), Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), and Digital Living Network Alliance (DLNA), where he contributed to technology enablers in the areas of mobile applications, messaging, real-time communications, Content Delivery Networking, content sharing with consumer devices, and IPTV.

Sergey has several patent applications, holds an M.Sc. degree in Engineering Physics, and is continuing his studies pursuing an M.Sc. in Applied Mathematics with University of Washington.

Poornima Magadevan, T-Mobile US, Inc.

Poornima Magadevan is a Principal Engineer with T-Mobile US, Inc. responsible for Internet of Things architecture and solutions. Poornima works closely with IoT solution partners to convert business problems into technology solutions across different IoT verticals.

She has contributed across technologies in the Telecom domain holding several patents.

Yun Zhang, Ericsson

Yun Zhang is a Product Development Leader at Ericsson Mobile Data Application Research & Development. He is responsible for driving Service Enablement product development especially Telco's Service Capability Exposure product at recent years.

Yun has filed several patents and has published articles in the areas related to Business Supporting System, Service Enablement, and Cellular IoT.

Sandeep Akhouri, Ericsson

Sandeep Akhouri is a Product Manager at Ericsson Mobile Data Application Research & Development. He is the Ericsson delegate for Open Mobile Alliance (OMA) Device Management & Service Enablement (DMSE) Working Group that is responsible for defining the Lightweight M2M (LwM2M) Technical Specifications.

Sandeep works closely with telecom operators and Enterprises in several different industry verticals, including Utility, Smart City, and Transportation.

He holds several patents and has published several articles at leading conferences on IoT, BSS / OSS and Analytics.